CCTV Policy

Date established:	May 2018
Updated:	March 2022
Reviewed:	Annually
Purpose:	This policy aims to set out MITSkills policy on the use of CCTV, and should be read in conjunction with our data protection and GDPR Policy

MITSkills is a learner centred private training provider working in the UK delivering training and skills valued by learners, employers, the community, and the UK economy.

We regard the lawful and correct treatment of personal information held by MITSkills as very important to successful operations and for maintaining confidence between ourselves and those whom we deal with. We therefore make every effort to ensure that personal information is treated lawfully and correctly.

MITSkills needs to collect a range of personal information in order to operate. This includes information relating to current, past, and prospective employees, suppliers, clients/customers, and others with whom we communicate. MITSkills requires this information to support the administration of its operation, and, in addition, it may occasionally be required by law to collect and use information of this kind to comply with the requirements of government departments for business data, for example. This personal information must be dealt with properly however it is collected, recorded, and used – whether on paper, in a computer, or on other material including CCTV – and there are safeguards to ensure this is in accordance with the Data Protection Act 1998. (Checked 2022)

We fully endorse and adhere to the principles of data protection, as detailed in the Data Protection Act 1998 and from 25 May 2018, the General Data Protection Regulation. The General Data Protection Regulation (GDPR) (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union. Please See our Data Protection /GDPR and Security Policy.

1. Policy statement

1.1. This Policy seeks to ensure that the Close Circuit Television (CCTV) system used by MITSkills is operated in compliance with the law relating to data protection (currently the General Data Protection Regulation (“GDPR”) and the Data Protection Act 2018 (“DPA 2018”)) and includes the principles governing the processing of personal data as set out in Appendix 1. It also seeks to ensure compliance with privacy law. It considers best practice as set out in codes of

practice issued by the Information Commissioner and by the Home Office (currently awaiting update). MITSkills therefore uses CCTV only where it is necessary in pursuit of a legitimate aim, as set out in clause 1.2, and only if it is proportionate to that aim.

1.2. MITSkills seeks to ensure, as far as is reasonably practicable, the security and safety of all students, staff, visitors, contractors, its property, and premises. MITSkills therefore deploys CCTV to: • promote a safe MITSkills community and to monitor the safety and security of its premises; • assist in the prevention, investigation, and detection of crime; • assist in the apprehension and prosecution of offenders, including use of images as evidence in criminal proceedings; and • assist in the investigation of breaches of its codes of conduct and policies by staff, students and contractors and where relevant and appropriate investigating complaints.

1.3 This policy will be reviewed annually by the Director of Operations to assess compliance with clauses 1.1 and 1.2 and to determine whether the use of the CCTV system remains justified.

2. Scope

2.1 This policy applies to CCTV systems in all parts of MITSkills West Byfleet and Brentford.

2.2 This policy does not apply to any Webcam systems located in meeting rooms or lecture theatres operated by delivery or ICT, which are used for the purposes of monitoring room usage, web meeting, presentations and to assist with the use of the audio-visual equipment.

2.3 This policy applies to all MITSkills staff, contractors and agents who operate, or supervise the operation of, the CCTV system including the Data Protection Officer and site support staff, and Directors.

3. Roles and Responsibilities

3.1 Managing Director has the overall responsibility for this policy but has delegated day-to-day responsibility for overseeing its implementation to the staff identified in this policy. All relevant members of staff have been made aware of the policy and have received appropriate training.

3.2 The Data Protection Office will be a director/or Company Secretary they are responsible for ensuring that the CCTV system including camera specifications for new installations complies with the law and best practice referred to in clause 1.1 of this policy. Where new surveillance systems are proposed, the Data Protection Officer will determine whether a prior privacy impact assessment is required.

3.3 Only the appointed maintenance contractor/or installer for MITSkills CCTV system is authorised to install and/or maintain it.

3.4 The Data Protection officer is responsible for the evaluation of locations where live and historical CCTV images are available for viewing via the network software. The list of such locations and the list of persons authorised to view CCTV images is maintained by Data Protection Officer.

3.5 Changes in the use of MITSkills CCTV system can be implemented only in consultation with MITSkills Data Protection Compliance Officer or Company Secretary.

4. System description

4.1 The CCTV systems installed in and around MITSkills covers building entrances, car parks, perimeters, external areas such as courtyards, internal areas such as social spaces, computer rooms, rooms with high value equipment, some corridors and reception areas. There are a number directly related to examination integrity and work on an individual computer work-station basis. Some cameras continuously record activities and some of the cameras are set to motion detection.

4.2 CCTV Cameras are not installed in areas in which individuals would have an expectation of privacy such as toilets, changing facilities etc.

4.3 CCTV cameras are installed in such a way that they are not hidden from view. Signs are prominently displayed where relevant, so that staff, students, visitors, and members of the public are made aware that they are entering an CCTV along with there is a CCTV. The signs also contain contact details as well as a statement of purposes for which CCTV is used.

4.4 The contact point indicated on the CCTV signs around MITSkills should be available to members of the public during normal business hours. Employees staffing the contact telephone number point must be familiar with this document and the procedures to be followed in the event that an access request is received from a Data Subject or a third party.

5. Covert recording

5.1 Covert recording (i.e., recording which takes place without the individual's knowledge): 5.1.1 may only be undertaken in exceptional circumstances, for example to prevent or detect an unlawful act or other serious misconduct, and if is proportionate i.e., there is no other reasonable, less intrusive means of achieving those purposes.

5.1.2 may not be undertaken without the prior written authorisation of Managing Director or in their absence, the Company Secretary. All decisions to engage in covert recording will be documented, including the reasons.

5.1.3 will focus only on the suspected unlawful activity or suspected serious misconduct and information obtained which is not relevant will be disregarded and where reasonably possible, deleted; and

5.1.4 will only be carried out for a limited and reasonable period consistent with particular purpose of the recording and will not continue after the investigation is completed.

6. Operating Standards

6.1 The operation of the CCTV system will be conducted in accordance with this policy.

6.2 Control room/ CCTV recorder

6.2.1 No unauthorised access to the CCTV recorders will be permitted at any time.

6.2.2 Other than Data Protection officer, access to the CCTV recorders will be limited to:

• persons specifically authorised by the Managing Director or Company Secretary.

• Company Directors.

• maintenance engineers.

• police officers where appropriate; and

• any other person with statutory powers of entry

6.2.3 Monitors for view CCTV are not to be visible to anyone not on the authorised list or specifically authorised by the Managing Director or Company Secretary.

6.2.4 Before permitting access to the CCTV recorders and monitors, staff will satisfy themselves of the identity of any visitor and existence of the appropriate authorisation.

All visitors are required to complete and sign the log, which includes details of their name, department and/or the organisation that they represent, the person who granted authorisation and the times of access to and exit from the CCTV storage.

A log of shall be retained setting out the following:

• person reviewing recorded footage.

• time, date, and location of footage being reviewed; and

• purpose of reviewing the recordings.

6.3 Processing of Recorded Images

6.3.1 CCTV images will be displayed only to persons authorised to view them or to persons who otherwise have a right of access to them. Where authorised persons access or monitor CCTV images on workstation desktops, they must ensure that images are not visible to unauthorised persons for example by minimising screens when not in use or when unauthorised persons are present. Workstation screens must always be locked when unattended.

6.4 Quality of Recorded Images

6.4.1 Images produced by the recording equipment must be as clear as possible, so they are effective for the purpose for which they are intended. The standards to be met in line with the codes of practice referred to at clause 1 of these procedures are set out below:

• recording features such as the location of the camera and/or date and time reference must be accurate and maintained.

• cameras must only be situated so that they will capture images relevant to the purpose for which the system has been established.

• consideration must be given to the physical conditions in which the cameras are located i.e., where appropriate additional lighting or infrared equipment may need to be installed in poorly lit areas.

• cameras must be properly maintained and serviced to ensure that clear images are recorded, and a log of all maintenance activities kept.

• as far as practical, cameras must be protected from vandalism in order to ensure that they remain in working order. Methods used may vary from positioning at height to enclosure of the camera unit within a vandal resistant casing.

6.5 Retention and Disposal

6.5.1 CCTV images are not to be retained for longer than necessary, taking into account the purposes for which they are being processed. Data storage is managed by the CCTV digital records and MITSkills overwrite historical data in chronological order to produce an approximate max 365 days rotation in data retention and then overwrite. CCTV used for exam verification purposes is held for not less than 90 to ensure exam integrity but can be held for up to 12 months.

6.5.2 Provided that there is no legitimate reason for retaining the CCTV images (such as for use in disciplinary and/or legal proceedings), the images will be erased following the expiration of the retention period.

6.5.3 All retained CCTV images will be stored securely.

7. Data Subject Rights

7.1 Recorded images, if sufficiently clear, are considered to be the personal data of the individuals (Data Subjects) whose images have been recorded by the CCTV system.

7.2 Data Subjects have a right of access to the personal data under the GDPR and DPA 2018. They also have other rights under the GDPR and DPA 2018 in certain limited circumstances, including the right to have their personal data erased, rectified, to restrict processing and to object to the processing of their personal data.

7.3 Data Subjects can exercise their rights by submitting a request to the Data Protection and Information Compliance Officer in the form contained in Appendix 2 along with evidence of their identity. MITSkills will charge an admin fee in relation to accessing and/or copying recorded images for data subjects where this is requested this will be £10 (Data Subject Access (DSA) request fee).

7.4 On receipt of the request, the Data Protection Officer will look at compliance with the request, and subject to clause.

7.5 The Data Protection Officer will communicate the decision without undue delay and at the latest within one month of receiving the request from the Data Subject.

7.6 The period for responding to the request may be extended by two further months where necessary, taking into account the complexity and number of the requests. The Data Protection Officer will notify the Data Subject of any such extension within one month of receipt of the request together with reasons.

8. Third Party Access

8.1 Third party requests for access will usually only be considered in line with the GDPR and DPA 2018 in the following categories:
• legal representative of the Data Subject.
• law enforcement agencies including the Police.
• disclosure required by law or made in connection with legal proceedings; and
• HR staff responsible for employees and university administrative staff responsible for students in disciplinary and complaints investigations and related proceedings.

8.2 Legal representatives of the Data Subjects are required to submit to MITSkills a letter of authority to act on behalf of the Data Subject and the subject access request form (please see Appendix 2) together with the evidence of the Data Subject's identity.

8.3 The Data Protection Officer will disclose recorded images to law enforcement agencies including the Police once in possession of a form certifying that the

images are required for either: an investigation concerning national security; the prevention or detection of crime; or the apprehension or prosecution of offenders, and that the investigation would be prejudiced by failure to disclose the information. Where images are sought by other bodies/agencies with a statutory right to obtain information, evidence of that statutory authority will be sought before CCTV images are disclosed.

8.4 Every disclosure of CCTV images is recorded in the CCTV Operating Logbook and contains:
• the name of the police officer or other relevant person in the case of other agencies/bodies receiving the copy of the recording.
• brief details of the images captured by the CCTV to be used in evidence or for other purposes permitted by this policy.
• the crime reference number where relevant; and
• date and time the images were handed over to the police or other body/ agency.

8.5 Requests for CCTV images for staff or student disciplinary purposes (or complaints purposes) must be authorised by the Data Protection Officer or Managing Director.

8.6 Requests for CCTV information under the Freedom of Information Act 2000 will be considered in accordance with that regime.

9. Complaints Procedure

9.1 Any complaints relating to the CCTV system should be directed in writing to the Data protection Officer promptly and in any event within 7 days of the date of the incident giving rise to the complaint. A complaint will be responded to within a month following the date of its receipt. Records of all complaints and any follow-up action will be maintained by the relevant office. If a complainant is not satisfied with the response, they may appeal to the Managing Director.

9.2 Complaints in relation to the release of images should be addressed Company Secretary and Managing Director as soon as possible and, in any event, no later than three months from the event giving rise to the complaint.

10. Useful links

The Information Commissioner's Code of Practice at the time of writing had been withdrawn a new code of practice by the Government was still in draft since Sept 2021 (March 2022).

The Home Office Code was withdrawn awaiting the new draft.

Appendix 1

Principles relating to the processing of personal data under the Data Protection Act 2018 and General Data Protection Regulation (GDPR).

Personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to the Data Subject;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the personal data are processed; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Appendix 2 CCTV Data request

Data Protection Contact Details	**Email:**	
	Tel:	
	Website:	
MITSKILLs-ICO Reference#		
Request Number: (MITSkills use only)		

Under data protection legislation (General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA 2018)) MITSkills must process personal data lawfully, fairly, transparently and for specified purposes (and not further processed in a way that's incompatible with those purposes). Exemptions apply which allow MITSkills to process (including disclosing) personal data in certain circumstances. However, there must always be a legal basis for the processing. MITSkills has compiled this form to support you in making your request for disclosure of personal data.

Please complete all relevant sections, giving as much information as possible. We will use it to:

• help us identify the data subject(s) and personal data relevant to your request,

• determine as a data controller whether or not we are able to process/disclose the personal data, and

• document the request and provide an auditable trail.

Unless MITSkills is satisfied that we are authorised to process the personal data by a legal basis in keeping with the data protection principles and data subject rights, or exemptions provided by the DPA 2018, we will be unable to disclose the personal data to you.

As part of ensuring CCTV data security, we will require two forms of ID we will accept Passport/Drivers Licence.

2. Details about the data subject

Please complete fully

Full name:		
Address: *(If relevant)*		
Previous address: *(If relevant)*		
Telephone number: *(If relevant)*		
Email address: *(If relevant)*		
Reference number: (i.e., staff/student number)	**Staff number:**	
	Student number:	
The data subject is a(n): *(Please tick whichever apply)*	**applicant or prospective student**	
	student or former student (including alumni)	
	employee or former employee (or contractor)	
	customer or another stakeholder	
Any other information to enable identification of the individual?		

3. Your details as a requester (if you are external to MITSkills)

Full name:	
Organisation:	
Role within your organisation:	
Email address:	
Telephone number:	
Two forms of ID signed copies (one photo ID) verified by counter signer see section (Please have counter signer sign and data on back)	

4. Your details as a requester (if you are an employee/ contractor of MITSkills)

Full name:	
Position held:	
Department/or name of contractor: *(Where applicable)*	
Line manager/: *(Where applicable)*	
Email address:	
Telephone/extension number:	
Two forms of ID signed copies (one photo ID) verified by counter signer see section (Please have counter signer sign and data on back)	

5.Legal basis for processing and applicable exemptions

All processing of personal data must have a legal basis. Please describe which bases apply to this request:	
Consent of the data subject Please send Signed evidence of consent	
Performance of a contract	
Comply with a legal obligation Please state what legal obligation (e.g., Safeguarding /Prevent/ Fraud Prevention etc)	
Protect vital interests	
Performance of a public task or exercise of official authority (Police investigation etc)	
Legitimate interests	

If you are requesting special category data, please specify the additional legal basis you are relying on (or exemptions in the Data Protection Act 2018): *(Mainly see Schedule 1 of the Data Protection Act 2018)*

If you are relying on exemptions in the Data Protection Act 2018 for the disclosure of personal data, please specify which exemptions: *(Mainly see Schedules 2-4 of the Data Protection Act 2018)*
If non-disclosure would be likely to prejudice the purposes for which you are requesting disclosure of personal data, please explain:

6. Details relating to the personal data you are requesting

Please include as much information as possible to helps us identify the personal data you're requesting.			
The personal data requested covers the following dates.			
From:		**To:**	

7. Signatures

All requests should be signed by the data subject, or the public authority, regulator making the requests

Signature:		**Dated:**	
Name and Position/Role or Data Subject:			
Counter signature: Confirming above signature and identity and agreeing to be contacted. *(e.g., manager, etc.)*		**Dated:**	
Name Position/Role: **Organisation**			
Contact of Counter Signature and email			

All enquiries about access to information should be addressed to the designated Data Controller/Data Protection Officer
Hani Zubeidi
Company Secretary and Data Controller
MITSkills Limited
12 - 13 Camphill Industrial Estate
West Byfleet
Surrey
KT14 6EW Tel 01932 341426 9 to 5 Mon to Fri Tel 07785 103001 (Other Hours)

Date Reviewed	10/03/22
Reviewed	Annually
Version Status	Approved
Approved By:	 Company Director: Date 10/03/22